Chapter 305

FUNDS TRANSFER

Introduction

The funds transfer operation can present a high degree of risk to a corporate credit union (corporate), its members, and the credit union industry as a whole. In light of the potential for material losses through error, inadequate controls, or fraud, it is imperative the corporate establish a strong internal control environment over funds transfer activities.

Security measures are for the benefit of the members, as well as the corporate. A corporate which operates under the impression its own internal security measures can be lowered simply because legal liability can be shifted from the corporate to the member is incorrect in its approach. If a corporate's inadequate procedures cause a member credit union to suffer a loss, the resulting adverse publicity could prove detrimental to the corporate credit union system (System) and credit union industry as a whole. Also, lax controls at any one corporate can simultaneously place many natural person credit unions at risk.

Methods of Affecting a Funds Transfer

Most corporates use the Fedline system to transfer funds in and out of their Federal Reserve Bank (Fed) account. Other methods include:

1. Sending funds through U.S. Central or another correspondent institution;
2. Sending funds through Open Door (see Appendix C for further discussion);
3. Manually communicating the request to the Fed by telephone;
4. Using Telex systems, such as Western Union; and
5. Using alternative software (such as YOJNA, IntraNet, Fedplu$, etc.) to access the Fed.

This discussion will primarily address controls over the Fedline terminal. When the corporate uses other methods and systems for effecting funds transfer, the scope of the examination will include a review of policies and operating procedures, internal controls, and segregation of duties surrounding the use of those systems and methods.

Since alternative software changes occur the examiner should request the user's manual from the corporate. The basic controls outlined in this chapter for the Fedline are similar to alternate software systems (e.g., dual controls, user IDs, security administration, physical security, transaction controls, and segregation of duties).

Managing the Fed Account

It is extremely important to ensure that:

1. Funds transferred are frequently balanced to the corporate's Fed account (at least twice a day for smaller corporates; more frequently for larger corporates); and
2. A detailed reconciliation of the Fed account is accomplished daily by an individual not otherwise involved in the funds transfer process.

A daylight overdraft occurs if the corporate's Fed account is in a negative position any time during the business day. An overnight overdraft occurs if the corporate has a negative balance at the close of the business day. Items settle throughout the day in the corporate's Fed account, resulting in fluctuating daily balances. If the corporate does not carefully monitor its account activity throughout the day, and reconcile the account at the end of the day, overdrafts can occur. Examiners will ensure the corporate has procedures in place to adequately monitor and maintain its Fed account balance. Overdrafts in the Fed account can indicate the corporate is having difficulties in meeting one of its primary roles, that of a liquidity facility.

If a corporate has incurred overdrafts during the examination period, the reasons for the occurrences should be determined. Most corporates are considered Banker's Banks under the Federal Reserve's Payment Systems Risk Policy. This policy states Banker's Banks should refrain from incurring overdrafts. They are usually required to post collateral to cover overdrafts if they do occur. The no-overdraft policy for Banker's Banks is primarily because these institutions are not required to maintain Regulation D reserves, and therefore, do not have access to the Fed discount window. Examiners should be aware if a corporate waives its Banker's Bank status, it then has the option of establishing overdraft cap limits as allowed by the Payments System Risk Policy.

Methods of Receiving Funds Transfer Requests

The payment order is the corporate's authorization to act on behalf of its member. As such, there must be controls in place to establish the authenticity and time of receipt of the funds transfer request order. These two elements are the primary components cited by the Uniform Commercial Code Article 4A (UCC4A) in establishing responsibility for executing the order. UCC4A has been established in most states and is incorporated into the Federal Reserve System's Regulation J. It establishes responsibility for improper or untimely processing of a payment order, or cancellation, from initiation to final execution of an originator's orders. UCC4A requires a security procedure acceptable to both the corporate and the member be established.

The most indispensable and sensitive components of funds transfer activities are the message systems employed to generate payment orders. Payment orders may be made in a number of ways ranging from manual (e.g., memorandum, letter, telephone, FAX, or standing instruction) to telecommunications systems.

Telephone Requests

Corporates may receive their funds transfer requests by telephone. It is extremely important the corporate take appropriate steps to ensure telephonic requests for funds transfers are made by an authorized individual.

Voice recognition is not an acceptable method for corporates to identify telephone callers requesting funds transfers. It is not reasonable to assume a corporate's employees are able to recognize the voices of many different employees from different member credit unions. Even the smallest corporates have multiple members using its funds transfer service, and most of those members have more than one individual authorized to make telephone requests to the corporate. Therefore, examiners will always take exception to this practice. The corporate should have an alternative means of verification or authentication.

Most corporates require the employee taking a funds transfer request audibly to repeat the information back to the member's employee making the request, in order to ensure all details of the transfer are understood and accurate. All corporates should implement this procedure.

Electronic Delivery

Corporates are now developing or purchasing systems for moving wire information via electronic receipt/delivery. It is extremely important the corporate take appropriate steps to ensure the accuracy of these transactions. Examiners must review these systems for system controls, internal controls, and adequate written procedures. The systems should also be reviewed on the information system side to verify adequate data security is in place and information is protected (e.g., firewalls, encryption).

Telex

Examples of larger companies providing telex services for funds transfers are Western Union, RCA Globe, ITT World Communications, and Money Gram. Telex systems do not include built-in security features. It is the responsibility of the sending institution to incorporate a test key in all instructions to a receiver to execute a payment order. If corporates operate terminals for any company using telex services for funds transfers, the surrounding controls will be closely reviewed. Controls over origination, data entry, release, and balancing should be the same or similar to controls over Fedline.

Recording Funds Transfer Requests

Most corporates use recording equipment to document funds transfer requests. This security procedure is useful because recordings can be used to settle disputes between the corporate and member credit unions; and because it deters initiation of unauthorized or fraudulent funds transfer requests on the part of corporate and/or member credit union staff.

Recording equipment generally is capable of recording several lines simultaneously. The cost of these systems can reach into the tens of thousands of dollars. However, since recording greatly reduces the risks associated with the funds transfer operation, this cost is usually justified.

Some corporates use desktop telephone recorders to reduce costs. However, they are not recommended as the employee can deactivate most, their tapes must be changed more frequently, and they require more maintenance.

Corporates should have written procedures and strict controls over access to the recording equipment including the following:

1. Physical security over the equipment and tapes;
2. The person responsible for changing and storing the tapes;
3. The person authorized to access and listen to the tapes;
4. Requirements for periodically checking the quality of recordings;
5. Retention period for the tapes (six to nine months is normal, but the corporate should review applicable laws and regulations); and
6. If desktop recorders are used, procedures should clearly state they cannot be deactivated.

Written (e.g., by mail or in person)

Mail and in-person funds transfer requests are not an expeditious method of communicating a funds transfer request, so these types of requests are seldom used. However, if a corporate accepts such requests, the signatures on all requests should be compared to signature cards on file prior to processing the funds transfer. For written requests, a callback to verify the authenticity of the request also should be performed. For accepting in-person requests, the corporate should require the individual sign a request form and compare the signature card to the signature on file.

FAX

Faxing funds transfer requests is not recommended for the following reasons:

1. It is difficult, if not impossible, to determine whether the signature on a FAX request is original or has been cut and pasted onto the document;
2. It is impossible to positively authenticate the source of the request, as FAX machines can be programmed to put a false identification line on the FAX message; and
3. The requester's password is compromised if the message is intercepted, or if unauthorized personnel view the FAX message after receipt.

Some corporates insist FAX requests are necessary because members want to expedite a transfer, but have difficulty in reaching the corporate due to busy phone lines. The examiner will always discourage any use of FAX machines to receive funds transfer requests. However, if the corporate is willing to implement stringent additional controls over FAX funds transfer requests, exceptions may be considered. The following supplementary controls must be in place:

1. Call back all FAX requests, including those for "pre-authorized" funds transfers, to the original requester and a second authorized employee of the member credit union;
2. Prohibit the writing of passwords, PIN numbers, or test keys on the Faxed documents; and
3. Ensure written funds transfer agreements of those members that send requests by FAX on a frequent basis clearly describe the limitations of the corporate's liability for accepting these requests.

Telegram or Telex

Telegram and telex messages should not be allowed for receipt of funds transfer requests for the same reasons FAX messages should not be allowed. Except for requests originating from some remote foreign location, use of the telephone for requests is just as expeditious, and it allows the corporate to use the security procedures previously described.

Electronic Mail (E-mail)

E-mail funds requests are acceptable as long as the corporate ensures that proper internal controls and security procedures are in place. Procedures must be designed to prevent the receipt of unauthorized messages, and to prevent interception and possible manipulation of authorized messages. At a minimum:

1. Passwords and controls should be on whatever system is used, both at point of origination and at the corporate;
2. Incoming messages must be accessible only by authorized corporate employees from the moment they are received (i.e., passwords and other machine-enforced controls);
3. A return message, confirming receipt of the request, should be sent to the member. This should be done in a manner which will ensure the return message is being sent to the member, even if the original message originated elsewhere; and
4. Missing required data should be resolved by telephone contact with the member.

Internally Generated Funds Transfer Requests

In addition to member funds transfers, corporates must move their own funds from institution to institution. Transfers for those corporates investing solely in U.S. Central are usually limited to a small number of destinations, such as the corporate's Fed account, commercial bank checking accounts, or U.S. Central. Since these requests are repetitive, they are likely to be established on Fedline as pre-

authorized (card) funds transfer requests. As long as controls are in place over creating templates for these pre-authorized transfers, as discussed on page 305-13, risk exposure is minimal.

When a corporate transfers its own funds to a non-repetitive destination (e.g., investment transfers), greater controls are required, as follows:

1. Requests should be signed by two authorized individuals in the investment department; and
2. The funds transfer department should perform a callback to the broker/dealer to verify the accuracy of the account number, amount, and other vital information before transmitting the funds. The telephone number and contact names should be from the funds transfer room's existing records, not from information supplied by investment department personnel. (See callback criteria on page 305-11.)

If either of these controls is not in place, the examiner will require their immediate implementation and document the deficiency as an examiner's finding.

Receiving Funds Transfer Requests from Foreign Countries

Due to complex security problems associated with foreign communications, acceptance of funds transfer requests directly from foreign countries is discouraged. Rather, the member credit union will be required to have its overseas branch relay the request to one of its offices within the United States, which should then contact the corporate.

If a corporate does accept foreign requests from a remote location (i.e., some third world countries), it may be received via telegram or telex, as that may be the only expeditious method of communication. Such messages should be received on a secured or "tested" telex system.

Controls over Passwords/PIN Numbers/Test Keys

The best way to identify callers and authenticate requests is by use of carefully controlled passwords, PIN numbers, or test keys. Password and PIN refer to a word or string of characters or numbers, which must be supplied by the user (requester) in order to make the request. A test key refers to the association of a code with the individual funds transfer request. The code is based on a sequential number, calculation, or algorithm, which is tied to the previous message

(request), which has been sent. The use of a "test key" is usually considered to be the most secure, since it is not as easily compromised.

Unless otherwise noted, the remainder of this discussion will use the term "password" to also include PIN numbers and test keys.

Allowing the same password to be shared by all employees of a member credit union is unacceptable. This practice increases the likelihood of controls being compromised and makes it more difficult to identify an individual and hold them accountable for their actions.

Some corporates assert written funds transfer agreements place legal responsibility for security problems, resulting from the sharing of passwords among the member's employees, solely on the member. Individual credit unions sometimes resist requests by the corporate to require separate passwords for each employee. Their typical objection is the inconvenience of assigning and maintaining a larger number of passwords. Such a position by the member credit union undermines the philosophy of the corporate that requires a high level of responsibility for security of passwords.

The method of assigning and communicating passwords to users must be properly controlled. The corporate should have written procedures for rectifying compromised password security by canceling the password and assigning a new one.

The password assignment and communication process must be independent of, and confidential from, operational staff who process funds transfers. The corporate must have security procedures over the process of communicating new passwords to or from individual users, as follows:

1. Passwords should be sealed individually in privacy envelopes which are sent to the member credit union's CEO or manager;
2. A separate verification form should be inside each envelope, which is signed by the user and returned directly to the corporate;
3. There should be controls in place at the corporate to ensure no passwords are activated until the verification is received from the original user; and
4. All forms should be destroyed under dual control after their receipt has been recorded.

If the users at member credit unions are allowed to select their own passwords, controls must be in place over the communication of passwords. In addition, the corporate should require use of alphanumeric passwords instead of words. Users tend to select easily

remembered words, or characters in a pattern. This increases the likelihood passwords will be compromised.

The corporate's funds transfer polices and procedures must require changing user passwords periodically, but not less than semiannually. In the case of an actual or suspected breach of security, passwords must be changed immediately.

Compromise of a password can occur in a number of ways. For example, an unauthorized individual may obtain a password from a rolodex file left exposed on a desk, or by looking over an employee's shoulder, and reading it off a computer screen. Taking specific precautionary measures can minimize risks. For example, Rolodex files should not be used for maintaining passwords. Corporate staff should never record passwords on funds transfer request forms, although there should be a notation area on the form where staff signifies the password was verified.

Passwords also can be compromised if employees discuss them in places were they may be overheard. Policies and procedures should require employees not discuss funds transfer operational information outside the funds transfer area. Furthermore, the use of speakerphones to take funds transfer requests from member credit unions is not acceptable.

Passwords may also be stored electronically, either on the corporate credit union network (CCUN) system, a LAN (local area network), or some other system. Some corporates use the "DCME" screen on the CCUN system to store member passwords. If passwords are stored on the DCME, access to this screen must be limited to those employees who receive or verify funds transfer requests.

There are also a number of computer applications, which are specifically designed to generate and store passwords. If such systems are located on the LAN or some other system, there should be security controls in place to limit access to the password applications. Regardless of where the passwords are stored, access to this information should be restricted.

Passwords will be stored in some form (hard copy or electronic media) at the corporate’s contingency site. These should be controlled appropriately, and there should be procedures in place to ensure a current set of passwords is maintained at the contingency site when passwords are changed.

Confirming Funds Transfer Requests

After a funds transfer request is received, but before the funds are actually transferred, the corporate should verify the authenticity and accuracy of the request. This is normally done by telephone callback; however, it can also be accomplished by E-mail or other secure means.

The most common method of confirming funds transfer requests is to make a telephone "call-back" to the member credit union. Telephones "call-backs" serve to:

1. Confirm the accuracy of the request;
2. Confirm the request is originating from an authorized individual, from an authorized location; and
3. Reduce the risk of errors or fraud.

Since passwords and telephone callbacks have somewhat different purposes, they are not substitutes for one another. Telephone callbacks should be performed by a different corporate employee than the one who took the request (telephone call) from the member. Preferably, the callback will be made to an employee at the member credit union other than the employee who originated the request. This is sometimes difficult in small credit unions with limited staff. If the corporate does not require the callback to go to a second employee of the member credit union, the examiner will determine whether the corporate has taken appropriate alternative actions to protect its own interests (i.e., a liability disclaimer in the funds transfer agreement, lower wire transfer thresholds, etc.).

The corporate's procedures should require callbacks be made to the member's telephone number as listed in the corporate's official records. A "speed dialer" used during the callback process is unacceptable.

Employees may attempt to deviate from established callback procedures to save time. For example, callbacks should not be performed by having the employee who received the funds transfer request, by putting the caller on hold, then having another employee confirm the information. This greatly reduces the effectiveness of the procedure, since this method does not ensure an authorized user was calling from a member credit union.

Call-back Criteria

There should be defined criteria in the corporate's procedures, outlining when callbacks are required. Common call-back criteria include:

1. All third-party funds transfers. The final recipient of a third party transfer is a party other than the member credit union or the corporate. The risk of loss is greater for third party transfers since the chance of recovering funds sent to a third party is less than recovering from the account of a member credit union;
2. All requests for establishing pre-authorized (card) transfers;
3. All funds transfers over a specified dollar amount; and
4. All investment funds transfers, which are not set up as a pre-authorized (card) wire transfer.

The criteria the corporate uses to determine which requests will be subject to callback should be maintained as confidential information. Knowledge of when a callback is performed would assist fraud perpetrators in evading the corporate's security procedures. If the corporate has publicized the criteria, the examiner will recommend that it be changed, and the criteria be kept confidential.

The corporate should also perform random callbacks on requests falling outside normal callback criteria. This will deter attempts by both outsiders and corporate employees to circumvent established controls.

Electronic Mail Confirmation of Funds Transfer Requests

Funds transfer requests may be confirmed using electronic mail ("E-mail"), instead of telephone callbacks. Although use of E-mail to communicate with members is not common, this will change rapidly as corporates seek to further automate the funds transfer process.

If the corporate uses E-mail for confirming funds transfer requests, it must take steps to ensure integrity and control over the process, by determining that:

1. The system and its software have adequate security safeguards in place, both at the corporate and at the member credit union; and
2. Any confirmation messages are transmitted to the system "address" listed in the corporate's records, and not sent to the address in the request message.

When other methods of confirming funds transfer requests are used, the examiner must use judgment in reviewing the controls surrounding these methods. The corporate must implement controls to minimize the risk of loss due to inadequate controls for confirming the accuracy and authenticity of a funds transfer request.

Post Telephone Audit of Funds Transfer Transactions

Some corporates have implemented an internal control procedure known as a "post telephone audit." In this procedure, an employee independent of the funds transfer operation telephones the member after completion of the transmissions of funds to confirm the authenticity and accuracy of the transaction.

Since the telephone audit is performed after the funds have been sent, it does not prevent errors or fraud from being detected before the funds are released. As such, the post telephone audit is not a substitute for telephone callbacks. The main purpose of the post telephone audit is to detect fraud. These telephone audits are usually performed on a sample basis, with the larger and more risky transactions (such as third party transfers) more likely to be included in the sample.

Pre-authorized (Card) Transfers

Many funds transfer requests processed by corporates are repetitive transfers, such as when a member credit union transfers funds to an investment account at another institution. Once established, the wiring instructions for repetitive transfers stay the same, except for the dollar amount. These transfers are called pre-authorized transfers, and most often, a template is prepared and utilized for recurring transfers. Pre-authorized transfers are also commonly referred to as "card" transfers because originally, institutions kept records of pre-authorized instructions on index cards.

Corporates usually handle repetitive transfers by establishing a template screen within the Fedline terminal. Once established, a password or PIN number is associated with the wiring instructions. When a card transfer request is received, the caller must only supply the password or PIN number, and state a transfer for a certain dollar amount is needed to the credit union's account at "ABC Bank."

The caller does not have to give an account number or the bank's ABA number, thus saving time and allowing the transfer to be sent more quickly and efficiently.

The corporate must have additional controls over the creation of card transfers, as follows:

1. Creation or editing of the templates should be performed by someone other than the employees who perform the "initiation" and "verification" functions on the terminal; and
2. If the template screen is for an investment transfer for the corporate's own funds, then creation or editing of those screens

should be performed by someone other than a corporate employee with investment authority.

Posting Funds Transfer Transactions

After the authenticity and accuracy of the request has been determined, the corporate is ready to post the transaction to the member's account. This should be done before the actual transmission, to ensure funds (or sufficient credit on a line of credit) are available.

Transmission of Funds on the Fedline Terminal

Funds transfer messages sent over the Fedline terminal must go through two processes before the message is transmitted:

1. Initiation involves entering the message into the terminal; and
2. Verification involves reentering all or part of the message into the terminal. The security options on the system allow the corporate to decide exactly which data fields within the message will be re-entered. Once the verification process is complete, the Fedline terminal automatically transmits the message, and the funds are transferred.

If the data entered during verification does not agree exactly with the data entered during initiation, an error will occur, and the message must be correctly edited before it will transmit. (The verifier also has the option of canceling the message completely). Since the data entered during verification must be exactly the same as entered during initiation, it is not feasible to require non-numeric fields to be reentered. Therefore, corporates usually require re-entry for only numeric fields. The critical numeric fields include:

1. The dollar amount;
2. The ABA number of the receiving institution; and
3. The receiving account number.

The accuracy of the transmission is dependent upon these numeric fields, not upon the words and names in the message.

The corporate’s operating procedures must require two different employees to perform the initiation and verification processes on the wire terminal. This should be reflected in the corporate's written policies as well as mandated by the machine controls set up for the funds transfer operating system.

Audit Copy of Printout of Fedline Terminal Messages

Messages on the Fedline terminal are printed and consist of three basic categories transmitted via Fedline. These are:

1. Outgoing transactions;
2. Incoming transactions; and
3. Miscellaneous messages.

The Fedline system assigns a sequence number to each message and each of the three message types has its own numbering sequence. All messages can be sent to the same printer, or different categories of messages can be sent to different printers.

Corporates generally use multiple-part paper on the Fedline printer. If multiple-part paper is not used, other adequate security arrangements must be established. One copy of the day's messages should be maintained in continuous form, from log-on to log-off. If the paper is broken (e.g., printer malfunction or paper supply runs out), a supervisor who is not a Fedline terminal operator should inspect the old and new continuous forms to ensure no messages are missing. A supervisor should initial the beginning and end of each form where the gap occurs.

Other Security Features of the Fedline Terminal

Local Security Administrator

The Local Security Administrator (LSA) is responsible for setting up new users on the local Fedline system, and setting the function levels of all users. The LSA is a powerful user and has the tools to bypass all security and effectively send a transfer with no supervision, if other compensating controls, such as prompt balancing and timely activity log review are not in effect. Internal controls and proper separation of duties are important in protecting the corporate from significant risk. The number of LSAs, usually between two to four, depends on the size and complexity of the corporate. The corporate should be able to justify the number of LSAs. The LSA should not have unaccompanied access to the funds transfer room. If a LSA does have access then the examiner must verify they do not have a host communications password established by the Federal Reserve.

User/Access Report Evaluation

The "User Profile Report" will be obtained for review during each examination. The examiner should observe the security administrator

obtaining this report from the Fedline terminal. The User Profile Report shows:

1. All authorized users;
2. Modules users have access to; and
3. Authorities users have within each module.

The examiner should identify all users of this report and determine authorization levels ensure adequate segregation of duties and internal controls.

Staff members should not have more than one user ID. Doing so would enable them to bypass the verification requirement by signing on with the first ID to enter transactions, and then signing on with the second ID to perform the verification.

In reviewing the User/Access report, particular attention should be placed on the following function codes:

1. LA Local Administrator;
2. FT Funds Transfer;
3. HC Host Communications;
4. ST Securities transfer function; and
5. ** The double asterisk allows a user to perform ANY FUNCTION.

HC (Host Communications Function)

Staff members assigned the LSA function should be restricted from the Host Communications (HC) function. A staff member with HC access could log on to the Federal Reserve host mainframe and transmit the funds transfer. Note: The staff member must have a host log on ID and security access on the Federal Reserve host mainframe to implement the funds transfer. There is no way to determine on the corporate's system if a user has host access. This can be determined only by calling the data security department of the Federal Reserve Bank. The listing or non-listing of the HC application under the user's ID is usually a good indicator of their host access ability. However, this method of determination is not conclusive since the LSA can use the Master ID to activate this application at any time.

** (Double asterisk) Function Code

The ** grants access to all applications on the menu except the LA function. The ** function code is a system default setting that should

be changed for all users whenever Fedline software is installed or restored.

Verification Fields

Staff members with Manager function level or the LSA have the ability to set the verification fields for funds transfers. Available options range from no verification of any field to required verification of every field. In between the two extremes, the Manager or LSA can select individual fields that would require second operator verification. Verification refers to fields that must be re-keyed by a second operator. If none of the fields have an "X" next to them, no re-keying is required by the second operator. However, a second operator will still have to provide sight verification by calling up the transfer on the screen and reviewing it. The Federal Reserve Board recommends, at a minimum, verification of the dollar field should be required, (i.e., marked with an "X" to indicate a second operator will have to re-key in the dollar amount). Some corporates may choose additional fields to verify, such as, account number, routing, number, etc. Refer to the Appendix 305A, for additional discussion of verification fields.

Supervisor Access Level

Wire room operating personnel should not have supervisory and manager level authority for the Fedline terminals located in their departments. This authority allows modification of screen defaults and message status overrides. This should be assigned to staff independent of daily funds transfer duties.

Assistant Supervisory Authority

This setting enables the user to change recurring wire templates. This level of security access needs to be restricted to very select staff. The individuals should not have access to the wire room except for supervised additions and changes to the recurring templates.

Physical Security

Location of the Fedline Terminal

The Fedline terminal should be located in a secured room dedicated solely for that purpose, with only authorized terminal operators and their supervisors having access. However, some (but not all) smaller corporates have limited space available and are unable to place the terminal in a secured room. In that case, the corporate should place the terminal in a low traffic area, but within sight of the workstations of all the terminal operators, and/or the operator's supervisor. Having

the terminal in a low traffic area will reduce the likelihood of unauthorized personnel gaining access to the terminal unnoticed. Having the terminal within sight of the workstations of all the operators, and/or within sight of the supervisor, could act as a psychological disincentive against any authorized operator initiating any unauthorized transaction. In addition, any other security controls available, such as a locking terminal cabinet, power-on passwords, etc., should be utilized when possible.

Number of Staff Present

At least two employees (that is, two employees who understand and have the authority to operate the Fedline terminal) should be present at all times when the Fedline terminal is operational. This should be a written requirement in the corporate's funds transfer policies and procedures.

Management should maintain a list of individuals authorized to be in the funds transfer room. Funds transfer room access should be restricted from unauthorized individuals such as maintenance staff, building management, etc.

Security of Telephone Lines

The corporate must establish controls to ensure all telephone lines are secure from eavesdropping. A breach of security could occur from either outside or inside the building. Security outside the building is the responsibility of the telephone company. However, security inside the building is the sole responsibility of the corporate. The examiner will ensure that:

1. The corporate's telephone system does not allow one extension to listen in on another extension (not usually a problem, as most telephone systems in use today no longer allow this to occur); and
2. The telephone switching panel is secure within the building.

The location and security of the panel is important since, with the aid of some relatively simple equipment, an unauthorized person could listen to a telephone line at the panel. The room containing this panel should be locked, and the key maintained by management of the corporate. When properly controlled, management will know when a technician needs access to this panel. Each technician's identification should be checked, and proper precautions should be taken to avoid any breaches of security during times when the panel is unsecured.

Encryption Key Devices

Fedline software is designed so the "encryption key" will deactivate if the terminal is jostled or moved. The Fedline terminal cannot be used again until the "encryption key" is reset.

Each Fedline user (financial institution) is provided with one of two devices to reset the Fedline encryption key. The examiner will determine which of these two devices (described below) was provided to the corporate, and then determine that proper physical security measures are taken to protect these devices.

Fedline Configuration Diskette

Some corporates are supplied by their Federal Reserve Bank with a computer diskette containing software, which will reset the encryption key in their Fedline terminal. For security reasons, the Fedline licensing agreement allows only two copies of the diskette to be maintained, one copy on site, and the other off site for use during implementation of its disaster recovery plan.

It is vitally important these two diskettes be kept in a very secure area (i.e., safe, safety deposit box, or locked fire proof cabinet), and access be closely controlled.

Two-Part Encryption Key Codes

Some corporates are supplied by their Federal Reserve Bank with a two-part code which, when entered into the terminal keyboard, will reset the encryption key in the Fedline terminal. The two halves of the code (each 16 digits in length) are to be maintained in the custody of two separate custodians in separate secure areas. The examiner will ensure this is being done. The examiner will also ensure the two custodians each maintain a copy of their half of the code in a secure off-site location, for use during implementation of the disaster recovery plan. In certain circumstances, one of the halves is maintained by the Federal Reserve Bank.

Master Password Backup Storage

There may be a situation when a local administration function needs to be performed, but there are no LSA's available. Therefore, the Master User ID password should be stored in a secure location, under dual controls, and be available for the operating personnel should the need arise. The Master User ID password use should be governed by sound internal control procedures and should be changed by the LSA after operating personnel have used it.

Written Policies and Procedures

The Corporate Examination Questionnaire - Funds Transfer, OCCU 305Q, lists questions regarding internal control practices pertaining to the funds transfer operation. Many of the questions specifically ask whether certain practices are addressed in the corporate's written policies and procedures.

Written internal control practices ensure consistent application and enforcement, even when there is a change of staff or management. It is also easier to hold employees accountable for internal control practices when they are in writing.

Fraud risk is increased if an employee or interloper has the opportunity to gain unauthorized access to the system and initiate or alter a payment transaction in an attempt to misdirect or misappropriate funds. The following reduces fraud risk:

1. Written personnel policies and practices should require, at a minimum, that:

    a) Vacancies in the unit be filled by internal transfers versus new employees, when possible;
    b) Relatives be restricted from working in the accounting or data processing departments;
    c) Individual responsibilities relating to security be in writing;
    d) Written organizational security procedures exist;
    e) Actions to be taken in the event of a security related incident be identified;
    f) Formal training programs be developed to emphasize security and control;
    g) Cross training exist within the unit;
    h) Rotation of responsibilities be unannounced;
    i) There be a minimum number of consecutive days of annual vacation;
    j) Reassignment out of the unit be made when a notice of resignation is given; and
    k) Terminated employees' sign-on ability is promptly canceled.

2. Management also must implement adequate physical security controls, including the following:

    a) Limiting access to computer and communications equipment to authorized personnel;

b) Protecting sensitive equipment within the secured area using access controls or device locks; and
c) Securing and limiting access to all data on portable media (tapes, disks, hard copies, microfiche, etc.).

3. Management should implement the following to minimize risk of data loss and/or destruction:

   a) Purchasing commercially available software products to access production data files;
   b) Limiting access to specified programs or user ID's by setting up each file for read-only or read-and-write access; and
   c) Employing encryption, authentication, and dial back data protection techniques when accessing data-in-transit from one participant to another.

4. Management must restrict access on software products using:

   a) Operator passwords to prohibit entry by unauthorized personnel;
   b) Automatic features to control the number of unsuccessful password attempts, password expiration, or designated periods of inactivity;
   c) Multi-level functions, by password, to require dual control and ensure no single employee can create and send transactions (e.g., restricting one operator to file creation and a second operator to file approval or transmission); and
   d) System administration level procedures require secondary approval to assign, initiate, and maintain passwords.

5. Reconciliation of entries on the Federal Reserve Statement must be performed to verify the work settled as anticipated. Proper segregation of duties dictates staff responsible for reconciling transactions not be otherwise involved in the funds transfer processing.

6. Internal audits of the funds transfer process occur on a periodic basis. Depending on the size of the corporate, audits could be performed internally or by a third party auditor. The size of the operation will dictate how often an audit of this area is performed. Examiner judgment should be used in this area.

OFAC Compliance with Wire Transactions

The Office of Foreign Assets Control (OFAC) of the Department of the Treasury administers and enforces economic sanctions against

targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals. While OFAC is responsible for promulgating, developing, and administering the sanctions for the Secretary of the Treasury, all of the financial institution regulators, including NCUA, cooperate to ensure financial institution compliance. The primary tool used is a listing by OFAC of "Specially Designated Nationals and Blocked Persons." The list changes regularly in response to changes in foreign policy. Corporate employees should be aware of the persons and entities on the list and assure that such accounts and transactions are blocked or rejected and properly reported to OFAC. Software is available to monitor wire transactions.

Examiners much ensure that the corporate is monitoring all funds transactions and that the listing or software used is up-to-date. A corporate must monitor all funds that are transferred and cannot assume that the member, U.S. Central, or the corresponding bank will review the transaction. Penalties can be assessed to each participant in the transaction. The corporate can receive additional information from the OFAC website at www.ustreas.gov/ofac/ or by calling 1-800-540-OFAC(6322).

Written Funds Transfer Agreement with Members

The corporate should have a written funds transfer agreement with each member. The agreement should outline the duties and responsibilities of each party. The agreement's purpose is to protect the interests of both the corporate and its members. Among other things, it should specify the responsibilities of the member concerning security features such as password/PIN numbers/test keys and telephone "call-backs."
The corporate should obtain the advice of its attorney in drafting the agreement. Written documentation, on the attorney's letterhead, should be maintained as an indication the attorney:

1. Reviewed the agreement;
2. Found it to be in compliance with applicable law;
3. Believes it is adequate to protect the corporate's interests; and
4. Believes it adequately addresses the issue of "commercially reasonable security procedures" as discussed in Article 4(a) of the Uniform Commercial Code.

In addition to the agreement, the corporate should have written documents from each member authorizing certain employees or officials to request funds transfers. This may be the ONLY document maintained in some corporates. In those cases, the examiner will take

exception and require development of a formal funds transfer agreement.

Personnel Policies for Funds Transfer Operation

Even a corporate with a sound internal control structure could hire individuals who could commit funds transfer fraud. Personnel policies should be in place, which will reduce the possibility of hiring such individuals. Having a responsible level of due diligence in the hiring process would help reduce this risk. Having these policies in writing will help to ensure they are consistently applied, and may improve the corporate's chances of collection if a bond claim is made against an employee.

The corporate should have written procedures addressing the review of references of funds transfer staff, including but not limited to:

1. Credit checks;
2. Bondability checks;
3. Prohibition checks; and
4. Criminal background checks.

The procedures should detail how background checks are completed. Procedures for verifying references and documenting the verification should be detailed. The corporate should be aware a bondability check only identifies whether the potential employee is bondable by the corporate's bonding company. (Normally, a corporate's bond is held by a company that specializes in credit union bonds.) These bondability checks attest only to bonding actions, which may have occurred as the result of previous credit union employment. If the individual committed previous crimes at some other type of financial institution, the bonding company may not be aware of these. Criminal conviction checks should not be limited to the state and municipal court records where the corporate is located. Federal court records should also be investigated, as many financial institution fraud cases are handled at that level.

The process of performing pre-employment credit and background checks is embroiled in a number of sensitive employment and privacy laws, many of which differ from state to state. Appropriate disclosures must be given to the applicant prior to performing credit and/or background checks. The corporate should always ensure the review and concurrence of legal counsel in determining its pre-employment policies and procedures.

The corporate should also have procedures, which address what steps should be followed when funds transfer personnel give notice of resignation, or are terminated. The procedures should include that immediately upon either occurrence, these individuals should be relieved of funds transfer responsibilities, and all access and authorization levels canceled both at the corporate and the Federal Reserve Bank. Employees should be transferred to a non-sensitive area after giving notice of resignation.

Contingency Planning for Funds Transfer Operation

Restoration of funds transfer operations is a critical factor in disaster recovery planning. If the corporate does not normally have a high volume of funds transfer activity, emergency funds transfer operations can be conducted manually via telephone contact with the Fed. If the corporate plans to use the telephone, staff must know the location of the back-up code word list.

If the corporate has a "mirror" Fedline terminal at the hot-site location, the corporate must ensure it is adequately secured. The examination scope will include review of Fedline user access and machine security settings for any hot-site terminals. Procedures and controls should remain the same at the "hot-site" as are used at the main office.

Security Safekeeping

Security Safekeeping Policy

The corporate's investment policy should explicitly detail all authorized methods for safekeeping securities. The offering of the safekeeping program may be found in another board-approved policy. Specific procedures should be in place to ensure adequate separation of duties and controls. Access control limitations should be similar to systems employed in the wire transfer area. Safekeeping policies and procedures should be written with risk assessment in mind. "Prevention control" rather than "discovery" should be the underlying theme and objective.

Security Safekeeping Environment

Corporates are normally involved in a safekeeping environment and typically safekeep investments through a program offered by U.S. Central. However, they often have other arrangements with banks, other safekeeping facilities, and/or the Federal Reserve. While assessing the internal controls of the safekeeping program is

important, evaluating the corporate's assessment of its safekeeping institutions is equally critical. The impact of an unauthorized security transfer can be similar to an unauthorized wire transfer by exposing the corporate to financial and reputation losses.

Internal Risk

Corporates typically minimize their risk by acting as a "pass-through" to an outside safekeeping institution. Contracts and procedures for member credit unions are often implemented to control the risk of potential legal liability or loss from a breach of security occurring outside of the corporate.

Review of Safekeeping Program

During the examination of a corporate that engages in a security safekeeping program, the examiner will review the program, policies, procedures, and internal controls. The examiner should document their analysis and conclusions of the program within the funds transfer memorandum.

In addition to network developed programs, the examiner may encounter "non-network" developed programs. Such programs may be developed in-house, by other corporates, or other outside financial entities. The examiner must have a complete understanding of the program and identify any potential risk to the corporate.

Separation of Duties

A written procedure needs to be on file, which describes the security transfer process and the individuals responsible. Segregation of duties in the movement of securities is a key internal control element. An adequate password system should be in place for members to initiate movement of securities. The same internal controls for the wire transfer area should be in place for security safekeeping.

The majority of security transfers are completed through U.S. Central. Requests for securities movement are initiated by electronic means. Access to the CCUN system and its input/transfer screen (DCHT) is password controlled. The examiner should determine that the CCUN verification function (DCHK) is not disabled. The examiner should

verify that the DCHT function is not set using a "Z" which bypasses the second verification for "free delivery" securities.

Other safekeeping relationships must be reviewed carefully to assess the level of control in place. Built-in security features offered by custodians should be fully utilized by the corporate.

Account Reconciliation

At any time during the day, the corporate should have the ability to identify and document the location of the participating member's securities. Safekeeping procedures should require that a reconciliation of the safekeeping account be performed daily and that all securities in safekeeping be reconciled at least monthly to a master database. Other reconciliation processes can be used by a corporate. Examiner judgment must be used to ensure that an adequate reconciliation process is in place.

Examination Objectives

The objectives for reviewing funds transfer activities are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control the risk in its funds transfer activities;
2. Assess management's guidelines for evaluating and monitoring funds transfer activities;
3. Determine corporate management and officials are adhering to established guidelines; and
4. Initiate corrective action when the corporate's funds transfer policies, procedures, practices, and controls are deficient.

Examination Procedures

See Corporate Examination Procedures - Funds Transfer.

Examination Questionnaire

See Corporate Examination Questionnaire - Funds Transfer.

References

1. NCUA Examiner's Guide;

2. FFIEC Information Systems Handbook, 1996 Edition;
3. Uniform Commercial Code, Article 4A; and
4. Open Door Training Reference.

Appendices

305A FEDWIRE DISCUSSION - Excerpts from the FFIEC Information Systems Examiner's Guide;

305B Copies of Sample Fedline Miscellaneous Security Settings and User Access Reports;

305C Examiner's Guide to Open Door; and

305D Examiner's Guide to Fedplu$.